Academic Research in Educational Sciences
ISSN: 2181-1385
DOI: 10.24412/2181-1385-2022-5-800-806

Volume 3 | Issue 5 | 2022
Cite-Factor: 0,89 | SIS: 1,12
SJIF: 5,7 | UIF: 6,1

ОБЗОР МНОГОУРОВНЕВОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ HONEYPOT

Шерзод Ражабоевич Гуломов
PhD, доцент, Тошкент ахборот технологиялари университети

Ҳусния Рустамовна Салимова
Магистр, Тошкент ахборот технологиялари университети

Шарофиддин Азимжон угли Бобомуродов
Бакалавр, Тошкент ахборот технологиялари университети

АННОТАЦИЯ

Каждый день множество людей по всему миру используют Интернет. Все люди в жизни проверяют электронную почту, просматривают веб-страницы в Интернете, покупают товары, играют в онлайн-игры и оплачивают счета в Интернете. но сколько людей понимают безопасность во время работы? Признают ли они вероятность заражения вредоносным программным пакетом под атакой? Даже какой-то вредоносный программный пакет распространяется по сети, чтобы пользователи могли столкнуться с множеством угроз. сколько пользователей признают, что их ноутбуки часто используются, поскольку технологии быстро развиваются, показывает новая единица области атак. Безопасность — очень важный аспект решения всех этих проблем. в этой статье мы будем использовать королевскую протею, чтобы сформировать реальную ситуацию. Король протеи может быть хорошо спроектированной системой, привлекающей хакеров. Привлекая хакеров в свою систему, вы сможете отслеживать процессы, которые хакеры запускают и запускают в вашей системе. То есть королевская протея может быть машиной-приманкой, которая выглядит как настоящая система для привлечения злоумышленников. цель приманок - исследовать, понимать, наблюдать и отслеживать поведение хакеров, чтобы сформировать более безопасную систему. king protea может стать отличным способом улучшить информацию директоров по сетевой безопасности и научиться использовать риторические инструменты для получения информации из системы жертвы. Приманки также очень полезны для будущих угроз, которые могут отслеживать атаки с использованием новых технологий.

Ключевые слова: Honeypot, безопасность.

ВВЕДЕНИЕ

Благодаря развитию веб-технологий люди будут просто искать данные и быстро отправлять сообщения. Однако, если вы в то же время не заинтересованы в базовой сетевой безопасности для быстрого роста сети, хакеры могут использовать сеть с некоторыми вредоносными программами, уязвимостями системы и программными слабостями. Сначала я хотел бы сформировать горшок для меда на машине. Все США пытаются найти брешь в системе безопасности, которая существует в системе. При формировании всего этого я хотел бы атаковать систему. Как только хакеры получат доступ к системе, они смогут взять на себя роль риторических следователей. Он использует полезный инструмент риторического расследования, чтобы проанализировать следы, оставленные хакерами, пытаясь найти изменения, которые произошли в системе жертвы. Также у нас есть склонность углубляться в тему рассмотрения вопроса о меркантилизме в системе. Директора по сетевой безопасности могут понять, что полезно создать несколько более безопасных систем для обнаружения угроз. Honeypot может быть системой, которая повреждает данные о черной шляпе. Король протеанов так же, как и другая система, которая содержит каталог, диск для конкретной системы, но его функции очень специфичны и совершенно разные. Таким образом, использование реальной системы — это просто известность между White Hat и Black Hat. Риск нельзя исключить, однако безопасность помогает уменьшить риск для вашей организации и защитить ваши ценные ресурсы. Остальная часть письма выглядит следующим образом: обсуждаются различные типы многообразия и объясняются многообразные приложения и разработка. Основной целью Honeypot является рассеивание вредоносного трафика от критических систем, получение раннего предупреждения о текущих атаках до атаки на критические системы, а также сбор информации о злоумышленниках и методах атак. Системы Honeypot широко используются в технологии обнаружения вторжений. Приманки можно определить как системы, используемые для отвлечения злоумышленников, злоумышленников, злонамеренных пользователей от основных систем. Приманки были разработаны с целью отвлечь злоумышленников от критически важных систем и получить важную информацию об их вредоносной деятельности. Во-первых, приманка — это компьютерная система. В нем есть файлы, каталоги, как в настоящем компьютере. Однако цель компьютера состоит в том, чтобы привлечь хакеров, чтобы

они побывали в нем, чтобы наблюдать и следить за их поведением. Таким образом, мы можем определить это как фальшивую систему, которая выглядит как реальная система. Они отличаются от других систем безопасности, поскольку они не только находят одно решение конкретной проблемы, но также могут применять различные проблемы безопасности и находить для них несколько подходов.

ЛИТЕРАТУРА И МЕТОДОЛОГИЯ

Исследовательские приманки в основном используются в военных, аналитических и правительственных учреждениях. они захватывают огромное количество данных. Их цель — найти новые угрозы и узнать больше о мотивах и технологиях Blackhat. Цель состоит в том, чтобы найти способ более надежно защитить вашу систему, не нанося прямой ущерб безопасности вашей организации.

Производственные приманки применяются в производственных сетях для повышения безопасности, используемой для защиты предприятий от атак. они собирают ограниченное количество данных, и в большинстве случаев используются менее интерактивные приманки. Поэтому администратор безопасности бдительно следит за передвижением хакеров и старается урезать ч er версии Nmap поддельные операционные системы не будут распознаны, и Nmap обнаружит проблему. Еще одним ограничением Honeyd являются сценарии, привязанные к разным портам. При обычном сканировании можно определить, какие порты открыты, но как только злоумышленник попытается подключиться к порту, он поймет, что служба является поддельной. Например, сценарий, используемый для веб-сервера, при подключении к нему с помощью telnet сервер должен отправлять ответы, но ничего не происходит. Другая проблема заключается в том, что нельзя понять, идет ли входящая атака на систему или нет. Потому что нет такой системы сигнализации, которая может дать понять, что происходит нападение. Сбор информации тоже не очень умный. В результате хакер может быстро понять, что с целью что-то не так, и прервать атаку. Даже непрофессиональные злоумышленники могут скомпрометировать приманку, не тратя на это слишком много времени. Потому что это очень популярные и простые в использовании известные методы, такие как Nmap. Для него не нужен дополнительный подход. Нашим вторым шагом было настроить приманку Nepenthes среднего уровня взаимодействия. Мы объяснили, как это

работает и как мы изучали это в части реализации. Однако мы обнаружили некоторые проблемы и с Nepenthes. Прежде всего, Nepenthes предназначен для захвата вредоносных программ через Интернет. В основном используется для этой цели. Таким образом, это должно быть реализовано очень быстро, поскольку угрозы для пользователей через Интернет резко возрастают день ото дня. Непентес не мог справиться с новыми угрозами. Поскольку появляются новые угрозы, а Nepenthes не обновляется, он не сможет перехватывать вредоносное ПО. Другая проблема связана с шеллкодом. Менеджер шеллкода должен подумать о шеллкоде и понять его. Поскольку новые угрозы не могут быть захвачены, новые эксплойты также не могут быть захвачены. Кроме того, поскольку мы изучаем проблемы и недостатки безопасности в нашем эксперименте, в структуре Nepenthes есть важный недостаток безопасности. Nepenthes не имеет защиты транспортного уровня. Безопасность транспортного уровня — это протокол, обеспечивающий безопасность связи в Интернете. Мы считаем, что это реальная проблема для развертывания приманки. Некоторые вредоносные программы существуют на порту 445, которые связаны друг с другом: «LSASS, PNP, DCOM, ASN1, ms06-070, ms08-067». Когда происходит такое вмешательство, мы также не уверены в ответах. Это создает большой беспорядок между модулями. (Шлёссер М., (2009)). На рис. 8.1 показаны атаки, наблюдаемые согласно Maheswari V. & Sankaranarayanan Dr.P.E. (2007).

ГОРШОК МЕДА:

• Honeypot может быть системой для сбора информации.

• Honeypots иногда размещаются за брандмауэром. King Protea в основном привык имитировать распространение сервисов и дыр, чтобы вызвать распространенность различных атак, атаковать информацию.

• Нарушитель со степенью младшего специалиста пытается войти в систему под ложным именем, администратор системы будет уведомлен.

• Как только кто-то попытается войти в систему, будет создан журнал со всеми входами.

• Даже если нарушитель проникнет в систему и перехватит информацию из информации, мы обманем его, предоставив поддельную информацию, это часто делает королевский протеа, однако нарушитель не вспомнит об этой поддельной информации. тем самым мы сохраним нашу систему и обманем злоумышленников.

• В то же время будут созданы журналы для того, чтобы вся информация о преступнике записывалась,

например, системная научная дисциплина, тип атаки, характер атаки, внешние следы и т. д., а также метод атаки для доказательства, которое может быть использовано. на любые действия.

ЗАКЛЮЧЕНИЕ

Безопасность — одна из немногих технологий, способных привести к серьезным изменениям. Следовательно, необходимо усилить безопасность устройств. В этой статье мы представляем способ борьбы со злонамеренными атаками и пользователями, использующими приманку. Организация может предпочесть использование приманки для обнаружения грубых элементов. Можно легко понять поведение злоумышленников, внедрив их. Поскольку риски в информационных технологиях растут день ото дня, требуются дополнительные усилия, чтобы приманка обеспечивала дополнительные функции безопасности и обнаружения, которые могут быть дополнительно расширены в стандартной версии передовой технологии. В этой статье мы изучили работу приманки и взаимодействие с злоумышленниками и вредоносными программами.

Во время этого теста автор делает вывод, что приманка и брандмауэр могут сотрудничать в сдерживании произошедшего инцидента, поэтому злоумышленник не может легко войти, потому что злоумышленник попал в созданную приманку-ловушку, поэтому сервер может работать безопасно. , и приманка успешно Обнаруживает подозрительную активность и захватывает IP-адрес злоумышленника и сохраняется в отдельной папке на ловушке-ловушке сервера.

Как и у всех технологий, у приманок есть свои недостатки, самым большим из которых является их ограниченное поле зрения. Приманки захватывают только действия, направленные против них, и пропускают атаки против других систем.

По этой причине безопасность эксперты не рекомендуют, чтобы эти системы заменяли существующие технологии безопасности. Вместо этого они рассматривают приманки как дополнительную технологию для защиты от вторжений на основе сети и хоста.

Преимущества, которые привносят приманки в решения по защите от вторжений, трудно игнорировать, особенно сейчас, когда начинают внедряться производственные приманки. Со временем, по мере распространения развертываний,

приманки могут стать важным компонентом операций по обеспечению безопасности на уровне предприятия.

Предлагаемая система

1. В предлагаемой нами системе Honeypot мы используем различные уровни безопасности для повышения безопасности системы Honeypot.
2. Использование генератора случайных чисел для генерации OTP
3. Неавторизованный человек не может здесь зарегистрироваться..
4. В предлагаемой системе мы записываем информацию о злоумышленнике, т. е. используемое имя пользователя, время входа в систему, время и дату выхода из системы.
5. Если неавторизованный пользователь войдет в систему, он сразу попадет в систему-приманку.

REFERENCES

1. «Обнаружение вторжений с помощью приманок» — Нирадж Бхагат M.Tech Центральный университет Джамму, кафедра. компьютерных наук и информационных технологий «2018IEEE
2. «Обнаружение и предотвращение вторжений с использованием сети Honeypot для облачной безопасности» Пурвика Сингх Неги, Адитья Гарг, Рошан Лал «2020IEEE
3. У. Такар, «HoneyAnalyzer — анализ и извлечение шаблонов обнаружения вторжений и сигнатур с использованием Honeypot».
4. Перевозчиков В.А., Шаймарданов Т.А., Чугунков И.В. Новые методы обнаружения вредоносных программ с использованием систем FTP Honeypot // Тр. 2017 IEEE Рус. Разд. Молодой рез. электр. Электрон. англ. конф. ЭлКонРус 2017. С. 204–207, 2017.
5. Э. Агирре-анайя, Г. Гальегос-Гарсия и Н. С. Луна, «Новая процедура обнаружения приманок с низким уровнем взаимодействия», том. 4, нет. 6, 2014.
6. Н. Провос, «Структура виртуальной приманки».
7. Диансях Т. М., Фейсал И., Пердана А., Сембиринг Б. О. и Синага Т. Х., «Анализ использования брандмауэра и одиночной приманки при обучающей атаке на беспроводную сеть».
8. И. Махмуд, «Информатика и системная биология. Использование Honeynets для обнаружения эксплуатируемых систем в беспроводных сетях», том. 11, нет. 2018. Т. 3. С. 219–223.

9. Honeypots: The Need of Network Security Navneet Kambow #, Lavleen Kaur Passi Департамент компьютерных наук, Shaheed Bhagat Singh State Technical Capmus, Ферозепур, Индия — Департамент компьютерных наук, Инженерно-технологический институт Арья Бхатта, Барнала, Индия
10. Кио Э., Чакрабарти К., Паццани М. и др. Уменьшение размерности для быстрого поиска сходства в больших базах данных временных рядов [J]. Journal of Knowledge and Information System, 2002, 3(3): 263～286.
11. Навроцкий М., Маттиас В., Шмидт Т.С., Кейл К. и Ш. Дж., «Обзор программного обеспечения Honeypot и анализа данных», 2000 г.
12. Ума Сомани, «Внедрение цифровой подписи с алгоритмом шифрования RSA для повышения безопасности данных в облаке в облачных вычислениях», 1-я Международная конференция по параллельным, распределенным и грид-вычислениям (PDGC-2010), 2010 г.
13. Ю. Бородовский, «Обзор возможностей литографии 2009», в Proc.Semicon West, 2009.